

- Operator: Good afternoon ladies and gentlemen, my name is Tina, and I will be your conference facilitator today. At this time I would like to welcome everyone to the Centers for Medicare and Medicaid Services National HIPAA Roundtable. All lines have been placed on mute in order to prevent any background noise. After the speaker's remarks there will be a question and answer period. If you would like to ask a question during this time simply press star then the number one on your telephone keypad. If you would like to withdraw your question press star then the number two on your telephone keypad. Thank you, Dr. Bernice Catherine Harper you may begin your conference.
- Bernice: Thank you. Good afternoon to those of you on the East Coast and good morning to those of you on the West Coast. I am delighted to be your moderator today for the 16th National HIPAA Round Table session. This call is being conducted by the Centers of Medicare and Medicaid Services, or CMS. As such today is the Health Insurance Portability and Accountability Act of 1996, or HIPAA, and specifically the administrative simplification provisions. We have a very full agenda today, so without further adieu I'd like to introduce our first speaker today Ms. Karen Trudel, acting Director of the Office of HIPAA Standards, Ms. Trudel.
- Karen: Thank you Dr. Harper. Good to have everyone on the call today. I can't believe that this is our 16th round table call. We started these calls in March of 2002 and certainly never expected them to be so well attended. I'm very pleased that we have been able to share information with thousands of people and answer hundreds of questions over the last two years.
Although several HIPAA deadlines have passed several others are rapidly approaching. It's been almost seven months since the deadline to comply with the electronic transaction and code substandard. Much progress towards compliance has been made but we all still have some work left to do.
Medicare implemented a contingency plan on October 16, 2003 that allows providers and other electronic billers to continue sending pre-HIPAA format electronic claims. However the contingency is temporary. Effective July 1, 2004 Medicare is modifying its contingency plan. The modification continues to allow submission of non-compliant electronic claim. However the payment of electronic claims that are not HIPAA compliant will take 13 additional days if they are received on or after July 6, 2004, and we'll provide a Medicare update later on this call.

In addition the compliance date for the Employer Identifier standard is July 30, 2004 for all covered entities except small health plans. The deadline for small health plans is August 1, 2005.

We are less than a year away from the deadline for complying with the HIPAA Security standards. The deadline is April 21, 2005 for all covered entities except small health plans. The security deadline for small health plans is April 21, 2006.

In January we published the final rule for the National Provider Identifier or NPI, the effective date for the NPI is May 23, 2005, at which time covered entities should be able to start applying for identifiers. The compliance date for the covered entities will be May 23, 2007 and May 23, 2008 for small health plans.

With all these deadlines coming up we will continue to conduct HIPAA round tables over the coming months to help you with your compliance efforts. Check our website for the latest information and notices of our upcoming calls. Again that website is www.cms.hhs.gov/hipaa/hipaa2.

For those of you who participated in our HIPAA round table calls before our format today will be a little bit different. The first part of the call will consist of a series of informational presentations. Then in the second part of the call CMS staff will address your questions related to electronic transactions and code sets, security, and unique identifiers. We ask that you hold your questions until all of the presentations are completed and we will open the line at that time, and now I'll turn the call back over to Dr. Harper.

Bernice: Thank you Ms Trudel. Our second presentation will be on HIPAA security. Our speaker will be Mr. Brad Peska of the Office of HIPAA Standards. Mr. Peska.

Brad: Thank you very much. I'm Brad Peska from the Office of HIPAA Standards. I work on the regulations team. I am responsible for providing information security expertise within the Office of HIPAA standards. I'd like to take a couple of minutes to talk to you about some security efforts that we're performing in the Office of HIPAA Standards, some efforts that are being performed by

outside industry groups, give a brief statement on the main points under the security rule, provide you with another brief statement on enforcement, and then summarize the presentation today. As Karen mentioned we have less than a year to go before the deadline for security compliance. Again that deadline is April 21, 2005 for all covered entities except small health plans, which have a compliance date of April 21, 2006. As we have learned from implementation of the privacy and the transaction and code set rules time frame will come up upon us very quickly. So what is the Office of HIPAA Standards doing to assist covered entities during their security implementation before the compliance date? As we've done with other rules we're helping covered entities by providing security outreach in a variety of means primarily through our website, which Karen stated is www.cms.hhs.gov/hipaa/hipaa2.

On this website we will be providing security FAQ's. There are some security FAQ's already existing on the website. We will continue to post security FAQ's in the near future, and add additional FAQ's as relevant issues come up in the industry as either struggling with or looking for more information to help them comply with the rules. We will also provide outreach via our "ask HIPAA" emails. We've received several questions on security issues through the "ask HIPAA" emails. We've been able to respond to most of those questions, any questions that we see which are repeated or frequently asked questions we tend to turn them into FAQ's, so this is definitely another means that you can provide, that we are able to provide you with additional outreach, and in addition we are also doing presentations like this one in other industry presentations at meetings or work group sessions to give more detail on the HIPAA security rules to covered entities that are out there or actively implementing.

We also have a presentation on the HIPAA administrative simplification website, which provides you with an overview of the rules, so there's another good reference that I recommend any of you who haven't seen it to go out there and download. So from an industry perspective we also have efforts that are being performed by various industry groups out there. Although we don't endorse some of the work products of the industry groups are providing, we do realize that they may be valuable resources to

covered entities while they implement the security standards, so I wanted to go through and at least highlight a couple of those organizations for you. The WEDI Strategic National Implementation Process or WEDI-SNIP has produced and will continue to produce several white papers on security issues. They are currently developing a white paper on risk analysis, which we feel will help covered entities as a reference moving forward with those activities, so continue to check the WEDI website for additional work products that they provide on various security issues under the HIPAA security rule. I also want to highlight the work of the National Institute of Standards and Technology, or NIST. NIST has also provided several special publications on a variety of security topics. The NIST special publications are available from their website. We do refer to NIST special publications in the final rule, but again we are not requiring covered entities to use the exact processes or approaches within those publications, we leave it up to covered entities to determine the relevance and the value of that content for their implementation approach.

I'd also like to announce that the National Institute of Standards and Technology has published a new draft publication for public comment on their website, that particular publication is called draft special publication 800-66, which is titled An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act Security Rule. As I mentioned it can be downloaded from the NIST computer security resource center draft publications website and I will try to give you that resource but if you don't get the whole web address definitely go to the NIST website, look for a computer security resource center and then draft publications, but the website it csrc.nist.gov/publications/drafts/html, so from that website you will be able to download a copy of that document, again it provides NIST view of how the various guidance documents that NIST has provided to the industry as a whole relate to the HIPAA security rules as well as how the FISMA, the Federal Information Security Management Act, relates to the HIPAA security rules. *(there is a link from CMS.HHS.GOV/HIPAA/HIPAA2 to this draft document as well)*

In addition to these industry groups I also want to refer you to other local, regional or national efforts, which may be developing various security products such as white papers, tools, or other best practice materials. Any of these resources that covered entities feel will assist them in their overall compliance program is encouraged, we encourage them to seek out those efforts, and again make their own decisions on how to best implement them. I'd like to take a couple of minutes here to make a couple of refresher points on the security rule itself.

Covered entities must comply with all applicable standards, implementation specifications, and requirements related to electronic protective health information within their environment. The security rule defines the administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of that electronic protected health information. A very important section in the rule is Section 164.306, which is titled the Security Standards General Rules. When covered entities are implementing standards and specifications for the administrative, physical, and technical safeguard sections, it's important that they are done in accordance with the security standards general rule section. We feel that this section will assist covered entities in making important compliance implementation decisions related to implementation of security measures. This section establishes that covered entities must ensure the confidentiality, integrity and availability of all electronic health information that that covered entity creates, receives, maintains, or transmits. It highlights the connection between security and privacy rules. It establishes the concepts of scalability and flexibility within the standards and provides a discussion of various factors that covered entities must consider when complying with the standards, including the importance of performing risk analysis and risk management process both of which are required standards, or sorry, required implementation specifications under the security and management process standard. This portion of the rule also allows covered entities to implement security measures for their environment that are reasonable and appropriate for their specific environment, that's another important concept to use throughout security implementation, the concepts of reasonable and appropriate for the specific covered entity. Some of the standards within the rule are required and covered entities must meet the full intent of the

standard.

We also use implementation specifications to further define a standard and allow covered entities additional flexibility in certain areas. Covered entities must go through an analysis of addressable implementation specifications. The required implementation specifications must be implemented, however on the addressable implementation specifications we allow covered entities to go through the analysis of whether they should, number one, implement the implementation specification if it is reasonable and appropriate for their environment, number two, if that addressable implementation specification is not reasonable and appropriate implement an equivalent alternative measure.

We also make the distinction in the general rule portion that maintenance of the security compliance program is needed. The security measures that are implemented for compliance within the covered entity must be reviewed and modified as needed to continue reasonable and appropriate protections within the covered entity. It's important to note that the standards are an ongoing process and we do expect covered entities to continue to maintain appropriate safeguards within their environment. We also want to point out that there's a very good reference within the security rule itself, it's appendix A, which is titled The Security Standards Matrix. It can be found on the last couple of pages on the Security Rule. This chart allows each of the standards and implementation specifications of the administrative, physical, technical safeguard sections. It also identifies the required or addressable designation of implementation specifications and this can be a very helpful matrix for the covered entity to use during their implementation process.

So now a couple of quick points around security enforcement-- Enforcement for the security rule will start after the effective date of the rule, April 21, 2005. We're working with the Office for Civil Rights, or OCR, since security and privacy overlaps, we expect security enforcement, much like transactions and code sets, to be complaint driven, and we will try to provide additional details on the security enforcement in the future.

In summary, we understand that covered entities may be at

different stages of implementation for the security standards, therefore it's important to continue to highlight the main points of the security rule as covered entities continue or begin to implement the securities standards. If you are covered entity that hasn't started, please remember that you have less than a year to do before the compliance deadline and performing your risk analysis, which is required, is good place to start. We do believe that the security standards represent good business practices many of which covered entities may already be doing to safeguard electronic protected health information within their environment.

Bernice: Thank you Mr. Peska. Our next presentation will be the National Provide Identifier and our speaker is Ms Patricia Peyton of the Office of HIPAA Standards.

Patricia: Thank you Dr. Harper. As Karen mentioned on January 23 of this year we published a final rule that adopted the National Provider Identifier, or NPI, as the standard unique health identifier for healthcare providers. The NPI must be used by covered entities in standard transactions to identify healthcare providers. As Karen also said the compliance date is May 23, 2007 for all covered entities except small health plans. Small health plans have an additional year to May 23, 2008. After the compliance date, a health care provider with an NPI will use only NPI to identify it as a healthcare provider in standard transactions. All entities that meet our regulatory definition of a healthcare provider, that's the one in section 160.103, are eligible to apply for and use NPI, both covered and non-covered providers may apply for NPI's but healthcare providers who are covered entities are required to do so to obtain and to use them by the compliance date and standard transaction. Non-covered providers who obtain NPI's do not become covered providers by virtue of the fact that they have an NPI. Nor are they required by the final rule to begin conducting electronic transactions just because they have NPI's. Entities who are not health care provides, such as taxi services, interpreters and others, are not eligible for NPI's because they don't meet our definition of a health care provider. Healthcare providers may apply for NPI beginning May 23, 2005, which is the effective date of the final rule.

The healthcare provider will complete an application in order to

get an NPI, which will be able to be done over the Internet or on paper. The application then goes to the National Provider System, or the NPS, where it's processed. The uniqueness of the provider is ascertained and the NPI is assigned. A healthcare provider under certain circumstances may still need to report its taxpayer identification number in a standard transaction to identify itself as a taxpayer. It would not use its NPI for this purpose because the NPI was not adopted as a taxpayer identification number. Similarly NPI's do not replace the functionality of the DEA number, which is used to identify a prescriber of controlled substances. Providers with NPI's therefore would not use their NPI where DEA regulations require the use of a DEA number. In the national provider system providers will be categorized as either individuals, which are doctors, nurses, other practitioners, or organizations, which include hospitals, labs, DME suppliers and group practices. It is possible that certain organization providers, such as hospitals and chain organizations will be able to obtain NPI's for subparts of themselves that function as healthcare providers. We went into some detail about this concept in the final rule and because we have a lot of things on their agenda I wasn't going to go into that in this presentation but we'll certainly answer any questions about it.

The NPI will be an all numeric identifier with a check digit in the tenth position. The check digit can help detect keying errors. There is no embedded intelligence about a provider within the NPI so you can't look at the NPI and know what kind of provider it identifies. The NPI is intended to be a lasting identifier that will not change over time. It has no expiration date, information that a health care provider puts on its NPI application might change over time and a covered provider is required to furnish updates of that information to the NPS within 30 days of the change. When this happens the NPS will update that providers record but the NPI won't change at all. A couple of words about group practices, the NPS can assign an NPI to a member of a group practice, like a physician who of course is an individual, and to the group practice itself, which is an organization. However the national provider system will not be capturing the fact that a certain doctor or other practitioner is a member of a group practice. The NPS will not be linking the practitioners NPI to the NPI of the group practice to which he or she belongs and the NPS will not be capturing all the

practice locations of the group practice. It will capture the mailing address and one practice location address, which is what it will be doing for any other organization provider. Health plans will have to continue to keep track of memberships and group practices and of the various locations of group practices if they need that information.

The NPI enumeration process does not take the place of a health plans provider enrollment process. These are two totally separate activities. The NPS will produce a variety of reports and statistics and will disseminate information to the health care industry in accordance with the system of records notice that we published in July 1998. CMS will be awarding a contract for the entity that we refer to in the final rule as the enumerator. This should happen sometime this summer. The enumerator will operate the national provider system and it will be interfaced with the health care industry, it will answer questions that providers may have about their applications, updates, the enumerator will also process requests for data from the National Data Provider System. Covered entities, particularly health plans, have all sorts of work to do to implement the NPI. Covered entities need to be looking at their business operations and identifying areas that will be impacted by the NPI. They need to determine the activities they must undertake in order to make changes to those operations as part of NPI implementation, and they need to start talking to their trading partners and their business associates to see how the implementation of the NPI will affect those relationships. It would be good to identify problem areas sooner rather than later and begin work on resolving them.

CMS will continue to post frequently asked questions on the CMS HIPAA website, which we've already given you a couple of times, we do add to those questions as appropriate. We will eventually be including a link to the NPI application form, once that form is ready and we will continue to work with the designated standards maintenance organizations, with WEDI, and with other industry groups to provide guidance and assistance in implementing the NPI. As always the HIPAA hotline and the "ask HIPAA" mailbox are available for you to send questions. Thank you.

Bernice:

Thank you Ms. Peyton. We'll now have a Medicare readiness

update from Ms Cathy Carter, Deputy Director of the Business Standards and Systems Operations Group in the Office of Information Services. Ms. Carter.

Cathy:

Thank you Dr. Harper. As of May 7th we have just over 83% of all Medicare incoming electronic claims coming in the HIPAA format. We've seen a steady increase in this percentage every week over the past few months, and although this is really good news and the percentage sounds very high, it means that we still have 17% of all of our electronic claims that are coming in on the old format. Now Karen mentioned at the beginning of the call that Medicare is currently operating under contingency plans and that is true and we will continue that plan for some period of time. However it's important that we keep making progress and that all the providers keep making progress because this contingency plan will have to end at some point. Karen also mentioned one of the measured steps that we have taken in that regard, and that is for modification of the contingency plan where Medicare will begin paying starting July 6th any claim that is an electronic claim not in HIPAA format, we would begin making those payments using the time frame that we use to pay paper claims, so what that means is any provider that continues to submit non-HIPAA electronic claims on July 6th we'll continue to pay those but the provider will have to wait at least an additional 13 days for their payment.

Now we are hoping that this measured step will assist providers in moving forward and moving on to the HIPAA format if they haven't done so already. We've been conducting extensive outreach about this provision. It's been in the press quite a bit, I think providers hopefully are aware of it and are taking steps to move to the HIPAA format in test like they need to. Another change that is going to take place on July 6th is that we are making some changes in the way we're editing claims for Medicare in order to ensure that we are sending out HIPAA compliant coordination of benefit transactions. About 50% of the claims that Medicare pays are sent on the electronic records for those claims are sent onto trading partners that we have agreements with and they become to those other payers an incoming claim, and so we are making some changes to make sure that what we are sending them is actually a HIPAA compliant claim, and there are three examples of changes that we are making. In one example, certain

data elements are now going to be required that had not been required by Medicare before. An example of that is a date of service for every line item even if there is no HCPCS code and only a revenue code. The second example of this kind of changes we're making, added changes we're making, is that we're not going to allow certain data elements to be submitted that we used to allow. An example of that is covered days on an outpatient claim. Finally the third example of changes that we are going to make is we're going to begin editing data in a way that we hadn't before. For example, Medicare does not use taxonomy codes, however if a taxonomy code is submitted to Medicare we will now (starting in July), begin editing that code for content to make sure that it is actually a valid code and will reject the claim if it's not a valid code. We've conducted extensive provider outreach about these changes and in fact prior to even sending out the instruction for the Medicare contractors to make these changes we solicited input from the provider community at large to make sure that they were aware of what we were planning and to get input on what these changes would mean to the providers, and we received very favorable responses that these are the kind of changes for the kinds of things that they are already familiar with in dealing with other payers.

Since the instructions were published back in March of this year we have published numerous articles, we have done talks on all kinds of open door forums with various provider groups, and we have advised all of those people doing HIPAA outreach efforts to include these issues, and I should have said at the beginning, but these particular changes that I'm talking about now only affect the institutional claims so they only affect the types of providers that submit institutional claims such as hospitals and SNFS and home health agencies, those are the major ones. I'll be glad to take questions; I guess when we are ready to –

Bernice: Thank you Ms Carter. Now Mr. Jamel Sparkes from the Office of HIPAA Standards will provide an update on HIPAA enforcements.

Jamel: Thank you Dr. Harper, happy to be here. My name is Jamel Sparkes of the Office of HIPAA Standards, more specifically I am on the enforcement team. I'm going to give you a brief overview of what we've seen as far as the complaints for transaction and

code sets (TCS) since October 16, 2003. Enforcement of TCS is a complaint driven process. To date we've seen about 125 total complaints, of that 106 have been transaction and code set related. The other 19 were complaints that came in, were complaints where the primary issue in the complaint was probably privacy or dealt with another agency or the office, and our process is to forward those on. I'm just going to give you a brief overview of the type of complaints we've seen, some complaint detail, and a brief summary of our investigation process.

Out of the 106 total complaints about 2/3rds, or 70, are involving the private sector. The others of course are public: Medicare and Medicaid. Out of the 106, we have 61 total open complaints and 45 closed complaints. Open complaints are those that they are still being investigated or perhaps the entity that the complaint was filed against is under corrective action plan. Most of the complaints are regarding claims and more specifically are about the impact to cash flow. What we did find is that most of the parties did attempt to resolve the issue with the entity that the complaint was filed against before coming to CMS; CMS was used as the last resort. In the past two months we are seeing a lot more complaints in regards to code sets but the issue remains the same; it has to do with reimbursement. Most of the complainers are small providers against health plans and/or clearing houses. The process that we use to manage the complaints is standard regardless of who the complainant is or who the entity is that the complaint is filed against. For the most part the investigation resides within the Office of HIPAA Standards but we do use external entities for technical interpretation, those organizations being Washington Publishing Company, or WPC, NCPDP and HCPCS. For the most part the complaints are settled through voluntary compliance if we do find a HIPAA violation. Most organizations are willing to work with us and with the complainant to reach a point of HIPAA compliance. We do have a couple of entities under corrective action plan, approximately eight or nine, there are not that many out there, but they also are willing to comply—just because they are under a corrective action plan (CAP) doesn't mean they are pushing back on OHS. We are using some of CMS's regional offices to manage the CAPs for private sector and Medicaid plans. One thing I forgot to mention in the beginning is that OHS does accept complaints on paper and via the Internet. The website for

the administrative simplification enforcement tool is www.htct.hhs.gov or via the CMS website under the HIPAA link you will find additional links for filing a HIPAA complaint but we are accepting paper and electronic complaints. Thank you.

Bernice: Thank you Mr. Sparkes. We certainly hope that you have found these informational briefs helpful and now we are going to allow time for questions. Operator will you give us the instructions for the questions and each person who would like to ask the question we'd like for you to give your name and your organization. Operator?

Operator: Thank you Dr. Harper. Ladies and gentlemen if you would like to ask a question you may do so by pressing star then the number one on your telephone keypad. Your first question will come from the line of Bob Harlot.

Bob: Hi I have a question for the NPI, was that Patricia that did that?

Patricia: Yes.

Bob: The subparts, I have heard recently that subparts are not a matter of a provider's discretion. If they're eligible for a special provider ID for a subpart they have to get one. Is that true?

Patricia: If an organization provider has a subpart that, for example functions as a provider and conducts electronic transactions, that covered provider must get an NPI for that subpart. If there are other federal regulations out there that require what would be a subpart of an organization to have a number to use for billing, like if some, if the federal regulations require that they have a Medicare billing number, as a subpart, then that covered entity should be getting an NPI for that subpart as well.

Bob: Okay, so if I'm a large hospital, an individual hospital but a large hospital and I have some outpatient clinics that operate semi-independently, we're independently enough that I would like them to be, that are all NPI, but in fact they bill under the same umbrella as you know within the same systems, or whatever, would that be allowed or required that they get, or are they allowed to get a NPI for those clinics and are they required to get an NPI for those

clinics, given—let's assume for a moment they don't have to have a Medicare separate billing number.

Patricia: Well if they bill anybody electronically or conduct any of the standards of the you know, HIPAA transactions electronically then they would, you would have to have that subpart get an NPI or get for the subpart, but its up to the organization provider to look at all of its components, its subparts, and see if they should have NPI's that they need to be identified in standard transactions etc.

Bob: Okay. I mean but if the clinics may not bill in any way independently from the hospitals computer systems may all be part of one big billing process but they function independent enough logistically that they want to have an independent NPI, and it sounds like you are saying to me they would have discretionary decision making there?

Bernice: We're having consultation in the room.

Patricia: What would be the reason be for having an NPI then?

Bob: It could be that they have different out patient contracts for this set of clinics with payers.

Patricia: Well but they wouldn't be identified in standard transactions; I don't know what they'd be using their NPI for. It's to identify a healthcare provider or a subpart that should have a number either required to, because it's handled transactions electronically or that some other federal regulation specifies that it needs a number to use for billing.

Bernice: Thank you, may we have the next question? Did you want the next question or do you want to go on?

Karen: This is Karen Trudel I want to clarify that for one moment. I guess I'm not seeing a purpose for a subpart to have a specific NPI if it actually is never identified independently in the course of the HIPAA transaction. The NPI for the larger organization could certainly be appropriately used in that way. Our requirement is simply that if the organization is a covered entity it would have an NPI and if it is subpart that needs to be identified it may have an n

NPI.

Bernice: Other comments in the room? Next question please.

Operator: As a reminder please state your name and your organization name.
Your next question will come from the line of Katherine Saleski.

Katherine: Hi I'm Katherine Saleski; I'm located in Meridian at East Mississippi State Hospital. I'd just like to get the website for on the security part for under the general rules, I mean computer resource, I did not get that website.

Bernice: Mr. Peska are you going to give that?

Brad: Sure, I'll give you that again and we will also provide a link to that website for you, we can call you and get that information to send it to you directly if you would like. That website again
www.cms.hhs.gov/hipaa/hipaa2

Bernice: Were you able to get it all?

Katherine: I did. Thank you very much.

Bernice: Thank you very much. Next question please?

Operator: Your next question comes from the line of Michelle Cornfeld.

Michelle: Hi, Michelle Cornfeld, St. Louis, Missouri, Sisters of Mercy Health care System. I mean calling in reference to the contingency plans. As CMS the regulator are they going to require health plans to list their contingency plans at the same time or do they have, do the health plans get to choose when they list their contingency plans?

Karen: This is Karen Trudel again, the listing institution, whenever Medicare makes the decision to list this contingency plan has no impact on other health plans. We are well aware that some health plans have lower percentages of compliance then we do and I'm sure some of higher percentages of compliance in terms of the number of inbound compliant claims they are receiving and so each health plan needs to make its own decision as to when the

appropriate time to lift the contingency and whether there might be any interim steps like the slow pay option that Medicare fee for service has already announced and will implement in July, so there's no cause and effect between those decisions at all.

Michelle: So CMS as the regulator is not going to put any pressure on the health plans to get their contingency plans listed?

Karen: What we said last July when we announced the contingency was that health plans need to be making a group based effort to bring their partners, their trading partners on board, and that as time goes by, as much time goes by it becomes more difficult to make an argument that good faith efforts are going on, but at this point I would say into the unforeseeable future the near future at least it appears to us that health plans are indeed making good faith efforts to test and bring their providers, the trading partners, into production, so at some point in future of course we expect that plans will begin to announce the ends of their contingency plans as appropriate.

Michelle: Thank you.

Bernice: Thank you, next question please?

Operator: Next we have Robert Starling.

Robert: This is Bob Starling from Cincinnati Children's Hospital and Medical Center. My question is regarding identifiers to be used on the 837 for referring physicians, and as Patricia said we're referring physician is associated with multiple practices they may have multiple EIN's and they may have multiple secondary identifiers from the same payer for each group practice they are associated with. Our question is on 837 does it matter which one of the physician's identifiers is provided for the referring physician or are we required to provide the respective identifier or EIN for the associated practice from which the physician's patient was referred?

Stanley: Let me just ask a clarifying question, are you talking about claims as of today or are you talking about after the national provider identifier is required?

Robert: Either one. Well as the implementation guide stated today you know, the secondary identifiers are still situational.

Stanley: The requirements for the secondary identifiers, let's say as of today, are probably set by each of the individual health plans, situational as the implementation guide requires. We expect when the National Provider Identifier is required in several years that there will be no secondary identifiers allowed simply to identify individual providers. The EIN number for tax purposes will still be required but given if provider has an NPI that's the only identifier that a health plan can ask for on a transaction as of the compliance date.

Robert: Well so until 2007?

Stanley: Yes.

Robert: What would be the answer then?

Stanley: The secondary identifier is allowed.

Robert: Do we have to provide the one associated with the respective practice from which they, the patient was referred or can we use any of their identifiers as long as it's on that's associated with that physician?

Patricia: Wouldn't that be up to the health plan? Whatever you are doing now. The NPI, you know, the compliance data is when all that may change.

Stanley: The secondary identifier is at discretion of the health plan.

Robert: Okay and for the tax ID number can we use any of their valid tax ID numbers?

Stanley: That again I think would be a matter of discretion for the health plan and also I guess the question of tax ID's, of the appropriate tax ID might be something that is affected by other requirements, other accounting requirements and such.

Robert: So if a companion guide does not address this matter it would seem that we have the latitude to use any valid number for that respective physician?

Stanley: Again I would discuss that with each single health plans.

Robert: Okay. Thank you.

Bernice: Thank you. You are welcome.

Operator: Next we have Chris Abel.

Chris: Hi this is Chris Abel; I'm with Nevada Medicaid. My question is on the National Provider ID, and my understanding when I read the regulations on that was that Medicare was going to coordinate the assignment of national provider ID's for their providers first. Is that correct, and then beyond that what is Medicaid's responsibility in trying to coordinate for their provider base?

Patricia: This is Pat Peyton. The final rules said that Medicare would be checking the feasibility of automatically enumerating some of the Medicare providers, but we don't know if we are going to do that yet or not but, and we can't make any requirements of Medicaid. We are going to have a cross walk made available to the health industry that would have the NPI and providers other identification numbers that are current on it for health plans including Medicaid.

Stanley: There is no responsibility on the Medicaid state agencies to enumerate their providers. The responsibility for obtaining a national provider identifier is that of providers, so the responsibility of the Medicaid state agencies is to get the national provider identifiers from their providers and use the appropriately in the standard transaction.

Chris: So then our only requirement kind of going back to what you said earlier from the business practice point of view was to ensure that our Medicaid management information system was modified to comply with the 10-digit field.

Patricia: That's correct.

Chris: Okay. Thank you.

Bernice: You are welcome. Next question please.

Operator: Next we have Martin James. Sir your line is open please go ahead.

Martin: Hi this is Heath Martin from Railroad Medicare contractor in Augusta, Georgia. What I was wondering is the NPI going to take the place of our existing provider files, our Pecos, is this going to take the place of those databases for us, and who will maintain it?

Patricia: The Pecos system is going to stay as it is, that's a Medicare enrollment system. That's a whole separate thing from the NPI enumeration system.

Heath: But it gives the provider a number that we use in our system.

Patricia: And it may still give you a number to use internally in your system, you know, but after the compliance date you will only see NPI's coming in on standard transactions. You will be receiving information from CMS centrally about how all this is going to work out.

Bernice: Does this give you the answer for now?

Heath: Not really.

Karen: This is Karen Trudel, I can add to that a little bit. The Pecos system is a system of enrollment in Medicare program as Pat indicated; it contains a great deal more information about Medicare providers than is required for the national provider identifier. Excuse me I'll finish in a moment.

Heath: I'm sorry.

Karen: The Pecos system does at this point assign a provider number because we were aware that the NPI was going to be some period of time down the road, and it will continue to do that. At the point in time where we begin to assign NPI's however, the Pecos system will hold the national provider identifier and that identifier will need to be recognized by Medicare systems when they receive an

incoming claim because that is what will be on the claim, so essentially the two systems mesh together, they do somewhat similar functions, complimentary functions and the data will match up behind the scenes.

Heath: And at some point during that time Railroad will go back to Pecos.

Cathy: This is Cathy Carter, let me just add that just like all other payers, Medicare is in the process now of evaluating the final rule and trying to determine exactly how the NPI is going to be implemented for Medicare purposes and there are meetings going on now and I think there will be opportunities for input by all or some at least of the Medicare contractor intermediaries and carriers and the system maintainers on how this process will work, so there's still some work to do to be able to answer the kind of questions that you are asking as well as other questions that need to be addressed in order to implement this rule.

Heath: Okay. Thank you very much.

Bernice: Thank you next question please.

Operator: Your next question comes from the line of Lisa Twinker.

Lisa: Hello this is Lisa Twinker from Blue Cross Blue Shield Association. We were wondering is CMS going to accept applications and issue NPI numbers to providers who reside and practice outside of the United States, if they need one to submit standard transactions to US health plans?

Patricia: --will be able to accept you know NPI's from foreign providers?

Lisa: Okay. They are not required to retain them though, correct?

Patricia: They are not required to do what?

Lisa: They are not required to obtain them because they are not covered entities is that correct?

Patricia: Well they could be covered entities.

Lisa: Even if they reside outside?

Patricia: I know we do capture a place of birth and an address of outside the USA. I would think some could handle transactions you know if they are near the border or whatever.

Lisa: Some of them are submitting 837 but they may not be covered entities. Is that correct?

Stanley: You're talking about like non-US citizens or foreign providers, like a Canadian provider or a South American provider that is dealing with the US insurance company?

Lisa: That's correct.

Stanley: I believe those would not be considered covered entities because they are not covered under US law.

Lisa: Correct. Okay.

Patricia: Then they wouldn't be required to get NPI's.

Lisa: They would be required to but you would accept an application if they tried?

Patricia: Sure.

Lisa: Okay. Thank you.

Bernice: You are welcome. Next question please.

Operator: Your next question comes from Andrew Frost.

Andrew: Yeah hi my name is Andrew Frost; I'm from IDX system corp in Burlington, Vermont. I just have a question about additional data requirements for the 837 professional format upcoming in July. You mentioned some requirements for institutional, can you tell me about any requirements for professional claims specifically around additional data and then secondly can you tell me what kind of requirements based on the employer identification number will be present in the 837 as well?

Cathy: To answer your first question of the additional data I was talking about only apply to institutional claims and there are no changes in edits for the professional claim as of July.

Andrew: Okay.

Cathy: On your second question I'm not sure I understood, do we need the question to be repeated—could you repeat the second question?

Andrew: Yeah well you mentioned at the beginning of the call that employer identification number standard is going into place and I was trying to get to understand it's relevance to the 837 professional claim and I honestly could find a part of the implement guide that would, that it would affect, so, I know it's going into effect in July and I just want to understand how you would interpret it's relevance to the 837 professional?

Pat: This Pat Peyton, the employer identification standard really isn't on the 837. That is for an employer acting in the role of an employer doing other transactions.

Andrew: Okay. That's what I thought I just wanted to clarify.

Bernice: Thank you. Next question please.

Operator: Your next question comes from the line of Grace Guthrie.

Grace: Yes my name is Grace Guthrie from Universal Care. On a note from the gentlemen that just spoke where can I find a list of the changes?

Cathy: The list of changes for the institutional claims, is that what you are talking about?

Grace: Yes, I mean the fields, like you mentioned the taxonomy codes and that you'll accept revenue code if HCPCS isn't there that's okay, so where do I find that information?

Robin Fritter: You need to look at the instructions that Medicare sent out in the follow up articles, are you familiar with the Medlearn Matters on

CMS's website for providers?

Grace: Oh okay, yeah.

Robin: If you look under the CMS website and click on the provider information page under Medlearn Matters there is a listing of every article that's been published, and then this one goes by the number of 3031.

Grace: Okay.

Robin: And you should be able to find it. That list for you-- all of the various requirements and hopefully you've gotten this information, you can either get it from the CMS website or off of the website for your individual intermediary that you send your claims to.

Grace: Okay thank you.

Bernice: You are welcome. Next question please?

Operator: Your next question comes from the line of Regina Gillus. Ms Gillus your line is open please go ahead. Your next question will come from Pablo Peramin.

Pablo: This is Pablo from Shepards Staff Christian Counseling Center in Sandy, Utah. I have two questions, you had mentioned earlier the employer identification standard that goes into affect July 30, '04, is this more then just having your EIN? I don't really know what that's about?

Patricia: No it's really not more then having an EIN if you are an employer, it's not you as a provider, it's the employer if they enroll or pay premiums, those types of transactions, most employers do have an EIN.

Female Speaker: If they have an EIN in place, is that basically what has to happen by July 30th?

Patricia: That's right. The EIN is their employer identification.

Female Speaker: Okay so as long as we have one we're set?

Karen: This is Karen Trudel, the requirements here is that the EIN be used in transactions where an employer needs to identify itself as such, and for instance the electronic enrollment, the 834 form, if that's being performed electronically then the EIN is the appropriate Identifier for use on that form, so for instance from perspective of submitting HIPAA compliant claims this really is not an issue.

Female Speaker: Okay, okay. Thank you. The other thing--

Bernice: -- did you have another question?

Female Speaker: In regard to the NPI you said subparts, and I would like a clarification of what that means, for example we're just a very tiny counseling center of just you know maybe three or four counselors, you have an administrative person and a billing person, would a subpart apply to us?

Patricia: No it wouldn't, and it would never be a human being anyway. No you wouldn't have any subparts.

Female Speaker: Okay, okay. Thank you very much.

Bernice: You're welcome. Next question please?

Operator: Your next question comes from Sandy Ahern.

Sandy: Hi thanks so much for taking my call, sorry I have a cold. I'm from Dr. Sectron and Dr. Larson's office in Nebraska. I just have a question, my software company was wondering if there is a deadline as far as when we are required to send our Medicare claims direct to our carrier?

Cathy: I'm not sure that I understand the question, you're not talking about format you are talking about whether or not you are allowed to use a vendor or billing agent to submit claims for you?

Sandy: Right now we go through another clearinghouse, which then forwards them on to Kansas and they are saying that we need to send our claims direct to Kansas now, and my software company is wanting to know when is the required deadline to meet that?

Cathy: I don't believe that that's a Medicare requirement, it sounds like that might be a requirement, change in the arrangement that you have with your particular vendor.

Sandy: Okay. No it's not the vendor.

Gary Kavanagh: Are you talking about submitting private side claims to Blue Cross Blue Shield of Kansas?

Sandy: No I'm talking right now we send out Medicare claims through Propar down to Kansas and then they send them over to CMS, you know to Medicare, and they told us that we have to send our Medicare claims direct to Kansas now not go through Propar.

Gary: So Propar is your vendor?

Sandy: No our vendor is actually McKesson. McKesson sends them through Propar and then Propar sends them to AFK to Kansas, and they are stating that we have to send them directly to Kansas and not go through Propar.

Cathy: Yeah, who's "they"? because again that's not – I don't believe that that's a Medicare initiated requirement. It sounds like a change in a relationship between you and the other entities that Medicare is not really a party to.

Karen: This is Karen, there are no requirements that Medicare claims need to be submitted directly, so what we're all suspecting is going on here is that there is some change in the business relationship between your vendor, that clearing house, and the Medicare carrier, and we would suggest, I think, that you might would want to talk with the electronic data interchange specialist at the carrier and try to get some clarification from that perspective.

Sandy: Okay. Thank you.

Bernice: You're welcome. Next question please.

Operator: Next we will have Gregory Grannon.

Gregory: Hi I'm Gregory Grannon. I'm at Delta Dental Plan of New Mexico, and I have question on the dental claim form and the code set, which is accepted and required for everyone to be using. On the last version of the American Dental Association claim form they have a column, which is area of oral cavity. Commonly for some code sets where either partial quadrant or a full quadrant are being billed, providers use terminology like UL, upper left, however in the CDT-4 book there is a section on international standards organization system, which list areas of the oral cavity, and which has a numerical nomenclature, which translates into the quadrants. As an example 30 designates the lower left quadrant, 40 designates the lower right quadrant. My question is in order to be HIPAA compliant do providers and health plans need to all be using areas of the oral cavity or is it acceptable for people to be using UL, which translates into this? Thank you.

Marie Margiotello: Well for Medicaid we can check with someone who's more familiar with the dental claim specifics and get back to you but my initial thoughts are that if the implementation guide is dictating that you use numerical digits in those fields on the form then it's probably not okay for you to be using the UL, or whatever you are use to. You need to go by whatever the guide specifies.

Karen: It appears that we have a need to get hold of our dental experts and look to see if there is any inconsistency between the 837 dental implementation guide and the CDT, and we will be glad to do that and that is going to take some research and we will have to get back to you.

Bernice: Thank you. Next question please.

Operator: Next we have Scott Erickson.

Scott: -- achieve health care technologies -- can you hear me?

Bernice: Yes.

Scott: My question is about the security rule. I've read the security rule on a number of times and I can find no provisions that talk about penalties or enforcement of the rules. And I noticed in looking at the provisions or the penalties in the privacy rule they specifically

apply only to the privacy rule, so I was wondering if somebody could just talk about penalties and enforcement of the security rule?

Lori: Hi this is Lori Davis. The Department of Health and Human Services will be publishing one enforcement rule that will take kind of an overarching approach to enforcement on the administrative simplification provisions, that would be for privacy transactions and code set security and the identifier standards. It probably makes sense rather than to have the Office for Civil Rights publish a separate enforcement rule and have CMS publish their own enforcement rule because we do have some overlap between privacy and security to have one enforcement rule that applies equally to all covered entities giving them all the same due process rights. The Department has drafted that rule. They are looking to publish at a later date and I unfortunately cannot give you a publication date at this point, but to tell you that the Department is actively working on it at this time.

Scott: Thank you.

Bernice: You're welcome. Next question please?

Operator: Next we have Leon Clason. Mr. Clason your line is open.

Leanette: It's Leanette Clason and we are with Inland Services in California. Could you define what a covered entities is and what a non-covered entity is? Thank you I'm going to go back on the speaker.

Patricia: A covered entity is a health plan, a health care clearing house, and a health care provider that transmits any data in electronic form in connection with the transaction for which we've adopted a standard. Anything that is not that would not be a covered entity.

Karen: This is Karen Trudel again on our website there is an excellent decision tool that allows individuals or organizations to go through a certain logic path and to determine whether or not they are or are not a covered entity under HIPAA, it's called the covered entity decision tool and again it's available on the CMS website.

Bernice: Next question please?

Operator: Next we have Christopher Sawyer.

Christopher: Hi yes, I'm Christopher Sawyer with the Scooter Store, and I'm calling concerning the Medicare part D region, or actually all of the Medicare part B contractors A-D. I'd like to ask a question concerning payers and their edit reports they transmit back to providers to indicate problem with claims that are not necessary related to HIPAA, as far as the formatting but with the contents of the claim not meeting the payers standard for entrance into their adjudication system, what we're seeing on our end are different reports between the DMERC contractors and a lot of our other carriers on commercial, as far as the formatting of those reports and the more, you know, the more payers that we submit claims to the more you know, the larger the problem gets. I was wondering if CMS will ever enforce this standard for reporting front end rejects prior to judicator so the larger providers won't be tempted to barrage payers with 276 transaction so they can ascertain whether or not the claim actually made it to the payer?

Cathy: This is Cathy Carter, the answer to that question is, and you know there is no standard, you've asked whether CMS will enforce one and I think that you know, if there is a standard in docket then certainly CMS will enforce it at that time, and I think that you know we, I'm hearing the input that you think it's an important aspect and it's some thing that we perhaps could consider in the future but there is no effort at this moment to standardize all the edit reporting primarily because we're in the process of implementing and helping all the providers to implement the standards that we do have to adopt at this time.

Christopher: Okay and we realize, you know, we realize everybody is still like on an early footing with this but we're seeing a potential problem going to, you know, emerging especially with on Part A very large hospitals and with part B large equipment carriers. You know when we send thousands of claims we need to know which ones didn't make it, so the 276 transaction we'd be very tempted to send gigantic batches you know daily to the carriers so that that way we can look at those reports and screen them to figure out whether or not they assigned a CCN number. To me if I was on the payer side I wouldn't want to have to have my systems drained all the time

you know just to do that whether as the reports they send to us now they are readable by human but not by computer.

Cathy: And are you saying that, I guess the question I have is this situation different now that we're in a HIPAA environment then it was before? What did you do prior to this? Everyone had a standard error report and it all looked alike and then with HIPAA all the sudden it got different?

Christopher: Well yes and no to that question. On the NSF format in our particular situation with DME we dealt with this problem by writing pricers for those reports and although those have changed with HIPAA and we saw this as an opportunity to address that issue.

Cathy: Okay—

Karen: --I think your point is well taken. You know there are going to be additional opportunities for the industry as we implement to come forward and say we've identified some areas where additional administrative simplification could take place where changes would be very valuable, and if your, if that's your experience we encourage you to do that. The National Committee on Vital and Health Statistics has periodic hearings and the Designated Standard Maintenance Organizations, the DSMOs, also do take in and consider potential changes to the standard.

Joy: This is Joy Glass there is an X12 error report, the 820 form but that just has not been prepared to be adopted.

Bernice: Thank you. Next question please?

Operator: Next will be Rhonda McClode.

Rhonda: Hi this is Rhonda and I'm also with the scooter store. I was calling in regard to the status of DMERC region B's backlog and an estimated date of resolution, in addition to that their ERN files are received like the day before their 835 files, do they have any estimated date of resolution on that?

Cathy: Have you talked with them because I don't think this call is really,

I don't think to get into specific carriers issues, I wasn't aware of that -- you're talking about a production problem?

Rhonda: Yes and they do not have an estimated date.

Cathy: -- for the 835?

Rhonda: Yes, and 837.

Cathy: You mean they are not able to accept any 837's and they are not sending out 835's?

Rhonda: They are accepting 837's however their 835's are going out about 24 hours later than the NSF files, and we're not getting any 997's from them.

Joy: When you said the 837, you are not getting any 997?

Rhonda: Right.

Joy: Okay which DMERC was this?

Rhonda: B. Administar federal --

Joy: Okay we'll check into this.

Bernice: Thank you very much. Next call please.

Operator: Next is Pamela Anderson.

Pamela: Yes hello this is Pamela Anderson, I'm with the Credit Bureau of North America, and forgive me all in advance if I'm taking up your time unduly but I'm not even sure I have the right forum here, however I am a third party, debt recovery specialist primarily for medical, well medical, dental and vision physicians, I'm finding myself more and more counseling them on how to obtain personal email certificates as a direct result of the 1996 HIPAA Act, and I'm looking for suggestions, advice, right now I have only one single website where these physicians can go to obtain personal email certificates, I wanted to know if there were any other resources, if this one resource is legal and official and if not what

the requirements are for them to transmit patient information's via email to our agency for debt recovery, and fall under the HIPAA Act requirements? Does that make any sense?

Brad: Yes, and from the securities standards standpoint under the HIPAA rules we can at least address that aspect. The HIPAA security standards section on technical safeguards addresses encryption of transmissions of electronic protected health information but that particular specification, implementation specification is addressable, which means covered entities must make the determination of whether certain transmissions such as in your example, email, must be encrypted when they send them if they contain electronic protective health information, but that is a decision that needs to be made by the covered entity—

Pamela: -- and in most cases that has been determined, and so that's why I'm finding myself in a position to work, you know, walk them through the obtaining personal email certificates, and I wondered if HIPAA had a division or somebody these physicians can go to make sure that their certified properly under the HIPAA ruling?

Brad: Not under the security standards under the HIPAA rules, and it's -- as far as my recollection and I can check into this, but there is no requirement for certification either especially in this circumstance in there. Although I cannot get into what the methods are there are other methods to encryption besides the one that you're providing so it could be a decision of a covered entity to maybe use another method besides a method that requires certification.

Pamela: If I might give you the website that I -- it's the only resource I have right now that I've been referring all my physicians to it is www.thawte.com, it looks as if it's a European based website, thawte, is the only resource I have right now.

Karen: Okay Brad will give you a call back and I want to reiterate that the security standards are by design based on the overwhelming public comment that we received extremely flexible in many respects, and that you know, while that is sometimes a problem for physicians to say well how do I do something it's also a, it's also a pro because there aren't specific requirements that the covered entities need to go out and purchase technologies so we're

essentially providing that kind of flexibility.

Pamela: Okay, yeah and on the other hand aside from protecting the physician, my client, I'd like to protect my company as well to make sure that we are following any HIPAA guidelines as a collection agency if you will, for you know to protect the patients confidentiality.

Karen: Right I understand that. Thanks so much.

Bernice: This will be our last question.

Operator: Your final question will come from the line of Alan Rosen .

Alan: Yes hi, Alan Rosen from WY Home health Services in New York City. It's my understanding that up until now taxonomy codes for home health providers needed to be filled in but basically had to have just a placeholder. Now I understand that starting July 1 we will have to have, we will not have to use it or have to have a valid taxonomy code, can we just leave it out, is that appropriate now?

Cathy: Taxonomy codes are not required by Medicare and so the only change that is going to be taking effect July 1 is that if you do submit a taxonomy code it must be a valid real code that exists on the file of valid codes, but you are not required to submit one, so yes you can leave it out and you can even leave it out now even prior to July 1st.

Alan: Right if we use a code that's a valid code but not necessarily relating to the claim as sort of a placeholder will that be accepted?

Cathy: Yes as long as it's a valid code.

Alan: Okay. Thank you very much.

Bernice: Thank you very much and now I want to thank you members of the staff for their participation, the conference is now concluded.

[END OF CALL]

